C Q R

Proceedings of Experts Workshop on Hardware & Software

Hosted by:

Rohde & Schwarz SIT

IEEE COMMUNICATIONS SOCIETY

ROHDE&SCHWARZ

Lucent Technologies
Bell Labs Innovations

Technical Sponsorship by :

Bell Labs, Lucent Technologies

IEEE COMSOC CQR

11 October 2006

Berlin, Germany

A. Resetko; K. Rauscher; R. Krock; J. Runyon

Agenda

9:00	Welcome, *Rick Krock, IEEE CQR 2007 Co-Chair*
9:05	EC ARECI Study, 8 Ingredient Framework, *Karl Rauscher, Bell Labs*
9:20	Message from Host, *Harry Kaube, Rohde & Schwarz SIT*
9:35	Introductions, *All*
9:50	Overview of 2 Ingredients, *Aleksei Resetko, Software & Hardware Workshop Chair*
10:00	Electronic Voting, *All*
10:15	Identification of Top Concerns, *All*
12:30	*Lunch*
13:30	Guidance for Addressing Top Concerns, *All*
15:00	Electronic Voting and Feedback, *All*
15:15	Next Steps and Closing Remarks, *Karl Rauscher*

ARECI Study

The aim of this study is to develop a forward-looking analysis of the factors influencing the ***availability*** *of electronic communication networks and of the adverse factors acting as potential barriers to the development of global networked economies by lowering their dependability.*

Information Society and Media
Directorate-General

8 Ingredient Framework

COMMUNICATIONS INFRASTRUCTURE

Power	Software	Payload	Human
Environment	Hardware	Networks	Policy

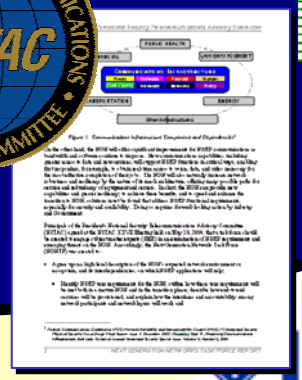
NRIC

WIRELESS EMERGENCY RESPONSE TEAM

NSTAC

NRSC

CQR



IEEE

IEEE COMMUNICATIONS SOCIETY

Workshop	Ingredients	Date	Location	Hosting Stakeholders
1	Power Environment	Tuesday October 3	Rome, Italy	Ministry of Communications, Italy
2	Network Payload	Friday October 6	London, U.K.	BT
3	Hardware Software	Wednesday October 11	Berlin, Germany	Rohde and Schwarz
4	Policy Human	Wednesday November 15	Brussels	t.b.d.

"These ground breaking workshops are bringing together experts for rigorous discussions on Europe's future communications networks. The systematic coverage of all eight of the fundamental ingredients of communications infrastructure will lead to improving the availability and robustness of our networks. These workshops are a ***necessary role model*** *for achieving consensus for Europe's ICT community. I am certain that the output of these workshops will provide bold, actionable and much needed guidance to the communications industry, member state governments and European Commission. I strongly urge the* ***continuation of this process****."*

- Dr. Luisa Franchino, Director General, Italian Ministry of Communications

5 October 2006

Ministero delle Comunicazioni

Experts Workshop
on Power & Environment
3 October 2006 - Rome, Italy

ROHDE & SCHWARZ

Message from the Host

Harry Kaube
Dipl.-Ing.

Head of Sales Germany
Rohde & Schwarz SIT GmbH

Welcome

Aleksei Resetko
Chair

Sr. Security Consultant, Lucent European Security Practice
Leader, EC ARECI study
Leader, Dubai Silicon Oasis Security & Reliability strategy
Certified Information Systems Auditor
Certified Information Systems Security Professional

Overview of 2 Ingredients

Hardware

Software

- Hardware frames
- Electronic circuit packs and cards
- Metallic and fiber optic transmission cables
- Semiconductor chips

- Applications
- Operating Systems
- Embedded systems
- Programmable interfaces
- Version Control
- Development and test
- Quality control
- Development life cycle

Intrinsic Vulnerabilities

Hardware

Software

VULNERABILITY
chemical (corrosive gas, humidity, temperature, contamination)
electric (conductive microfiber particles – carbon bombs)
radiological contamination
physical (shock, vibration, strains, torque)
electromagnetic energy (EMI, EMC, ESD, RF, EMP, HEMP, IR)
environment (temperature, humidity, dust, sunlight, flooding)
life cycle (sparing, equipment replacement, ability to repair, aging)
logical (design error, access to, self test, self shut off)

VULNERABILITY
ability to control (render a system in an undesirable state, e.g., confused, busy)
accessibility during development (including unsegregated networks)
accessible distribution channels (interception)
accessibility of rootkit to control kernal/core
developer loyalties
errors in coding logic
complexity of programs
discoverability of intelligence (reverse engineer, exploitable code disclosure)
mutability of deployed code (patches)
incompatibility (with hardware, with other software)

Workshop Notes

Top Concerns - Software

1. The development of security comes after the development of features
2. The speed of the transfer of knowledge from experts to the public, and the availability of tools to the public allows more people to hack
3. There is an increased risk of attack to distributed middleware due to the distribution and interconnectivity of networks
4. The current concern is that people are depending on security by controlling information (i.e. security by obscurity)
5. Protection and fault tolerance in run time environments is insufficient, especially against malicious code
6. There are a growing number of software layers which result in additional complexity, and requires coordination among applications and definition of interfaces
7. Different implementations of same security functions on different platforms (e.g., different file systems, different memory allocation) results in an inability to abstract security functions

Workshop Notes

Top Concerns – Software

8. Quality of software cannot be assured because of economic pressure, time to market, and short term business opportunities
9. There is a lack of awareness and acceptance of security issues by the public
10. Integration of security functionality into the interface may decrease functionality and performance even while it increases acceptance
11. Monopolistic position of particular software vendors allows them to constrain options of users (e.g., economic, technology)
12. Custom developed components may comply with standards but may still not be interoperable
13. There is a relation between security in homogeneous systems and dependability in heterogeneous systems, which presents competing interests
14. Many of the standards are overloaded with options which introduce complexity and may result in incompatibility

Workshop Notes

Top Concerns – Software

15. There is a conflict between security protections and the need for lawful intercept and monitoring of system insights and architectures by government
16. There is no common understanding between governments regarding the required level of security (i.e. the internet is international while regulations are national)
17. When using third party components, it is difficult to determine what security standards they are following, and the level of security throughout the supply chain (i.e. cascading vulnerabilities)
18. There is a lack of application of formal verification methods for assuring correct behavior of software components, applications, and systems
19. It is more difficult to trace malicious programmers because of off-shore outsourcing, and therefore less of a deterrent
20. Off-shoring may expose differences of culture and understanding throughout the software supply chain
21. Version upgrades may introduce incompatibilities
22. Incumbents may use interoperability constraints as a barrier to other carriers
23. Software vendors are not interested in making their products interoperable

Workshop Notes

Top Concerns – Hardware

24. Telecommunications hardware vendors may not be interested in making their products interoperable
25. The development of security comes after the development of features
26. Different implementations of same security functions on different platforms (e.g., different file systems, different memory allocation) results in an inability to abstract security functions
27. Quality of hardware cannot be assured because of economic pressure, time to market, and short term business opportunities
28. There is a lack of awareness and acceptance of security issues by the public
29. Integration of security functionality into the interface may decrease functionality and performance even while it increases acceptance
30. Monopolistic position of particular hardware vendors allows them to constrain options of users (e.g., economic, technology)
31. Many of the standards are overloaded with options which introduce complexity and may result in incompatibility
32. There is a conflict between security protections and the need for lawful intercept and monitoring of system insights and architectures by government

Workshop Notes

Top Concerns – Hardware

33. There is no common understanding between governments regarding the required level of security (i.e. the internet is international while regulations are national)
34. When using third party components, it is difficult to determine what security standards they are following, and the level of security throughout the supply chain (i.e. cascading vulnerabilities)
35. It is more difficult to trace malicious hardware designers because of off-shore outsourcing, and therefore less of a deterrent
36. Off-shoring may expose differences of culture and understanding throughout the hardware supply chain
37. Incumbents may use interoperability constraints as a barrier to other carriers
38. Hardware isn't being protected against sophisticated, military-like attacks (i.e. energy attacks, not physical)
39. As hardware becomes more sophisticated (i.e. smaller with more functionality), it becomes more vulnerable to the physical world
40. Hardware theft (including power lines) is becoming a bigger concern
41. Smaller hardware is easier to lose or be stolen
42. Cascading failures of hardware are not manageable in the traditional way

Workshop Notes

Guidance for addressing Top Concerns

21 Version upgrades may introduce incompatibilities.

Guidance:

- There should be penalties for failure to deliver or for problems caused. Lack of maturity of the ICT sector is why this doesn't exist.
- Software should be extensively tested in experimental and laboratory environments prior to deployment, both by the vendor and by the consumer.
- Software should be tested by someone other than the developer.
- Vendors should "consider" external certification – or not
- There is concern that there could be different requirements for small and big industry participants
- Market forces may regulate possible incompatibilities (e.g., BASEL 2, SOX)

Workshop Notes

Guidance for addressing Top Concerns

6 There are a growing number of software layers which result in additional complexity, and requires coordination among applications and definition of interfaces.

Guidance

- There is a need for execution environments that can tolerate malicious faults (i.e. implement standards in a more resilient way)
- Simple interfaces between software layers are preferred over complex interfaces (e.g., inheritance of properties)

Workshop Notes

Guidance for addressing Top Concerns

17 When using third party components, it is difficult to determine what security standards they are following, and the level of security throughout the supply chain (i.e. cascading vulnerabilities)

Guidance

- Testing in static environments has limited usefulness, and must be combined with testing in a dynamic environment to uncover cascading vulnerabilities.
- The quality assurance procedures of the vendor should be transparent.
- Establishing a standard certification would help improve quality (e.g., ISO 9000 certification)

Workshop Notes

Guidance for addressing Top Concerns

34 When using third party components, it is difficult to determine what security standards they are following, and the level of security throughout the supply chain (i.e. cascading vulnerabilities).

Guidance

- Easily identified system boarders would allow insertion of probes to detect suspicious activity (also applies to software)
- A common international understanding of security standards must be detailed enough to guarantee security quality.
- Given the option, it is advisable to use certified products (common criteria)

Workshop Notes

Guidance for addressing Top Concerns

42 Cascading failures of hardware are not manageable in the traditional way.

- They are unpredictable so traditional models of reliability may not apply. Normal failure distribution may not apply

Guidance

- Research on failure modes of interconnected hardware is needed
  - EMC vulnerabilities, transmission lines, logical failures
- Vendor heterogeneity would limit the area of failure
- Plans to recover from cascading failures must be established before the event occurs
- Preventative measures should be established rather than simply corrective measures

Workshop Notes

Guidance for addressing Top Concerns

27 Quality of hardware cannot be assured because of economic pressure, time to market, and short term business opportunities.

Guidance

- Contractual financial penalties should be established to cover hardware that does not perform as advertised
- Reduction of functionality on core features can allow the core functionality to be developed with higher quality, and additional functionality can be added later.
- More effort should be put into prediction of technology and features which allows vendors to deliver to the market earlier.

Next Steps

IEEE CQR to Publish Proceedings on Web (October 2006)
Workshop 4 (November 2006)
Public Workshop (January 2007, Brussels)
ARECI Study Final Report to European Commission (February 2007)
IEEE CQR International Workshop (May 2007, Florida)

Participants

Aleksei Resetko, Lucent Technologies

Karl Rauscher, Bell Labs & IEEE CQR

Ralf Guhl, Rohde & Schwarz

Marc van Kasteren, KPN

Per Mellstrand, Blekinge Institute of Technology

Roberto Oya Luengo, Lucent Technologies

Harry Kaube, Rhode & Schwarz

Gregor Kutzschbach, Bundesministerium des Innern

Stefan Ritter, BSI

Anastasius Gavras, Eurescom

Jonathan Wegener, McAfee

Carlos Saiz, Lucent Technologies

Rick Krock, IEEE CQR & Bell Labs

Jim Runyon, Bell Labs

Roberto García Blanco , Lucent Technologies

Jan Moenikes, Initiative Europe Netzetreiber

Alistair Munro, University of Bristol